PathCleanupSpec

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita[1]]

Copyright © 2007 Cigital, Inc.

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4040 bytes

<table>
<tr><td>Attack Category</td><td>Malicious Input
Path spoofing or confusion problem</td></tr>
<tr><td>Vulnerability Category</td><td>Buffer Overflow
Unconditional</td></tr>
<tr><td>Software Context</td><td>File Path Management</td></tr>
<tr><td>Location</td><td>shellobj.h</td></tr>
<tr><td>Description</td><td>The destination string buffer for the PathCleanupSpec() function must be long enough to hold the return file path.

The PathCleanupSpec() routine removes illegal characters and, if necessary, converts filenames to 8.3 format on drives that do not support long filenames. The result is not necessarily predictable, so ensure that the destination is MAX_PATH in length.

Note: This routine appears to be deprecated and is not in newer versions of the API.</td></tr>
<tr><td>APIs</td><td><table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>PathCleanupSpec</td><td></td></tr></table></td></tr>
<tr><td>Method of Attack</td><td>Attacker can trigger a buffer overflow if the destination buffer is not long enough to hold original path name. If the attacker passes in a path name longer than the destination buffer, the buffer will overflow.</td></tr>
<tr><td>Exception Criteria</td><td></td></tr>
<tr><td>Solutions</td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>When PathCleanupSpec() is used.</td><td>The second parameter, pszSpec, must be at least MAX_PATH</td><td>Effective.</td></tr></table></td></tr>
</table>

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	characters in length.
Signature Details	int PathCleanupSpec(LPCWSTR pszDir, LPWSTR pszSpec);

Examples of Incorrect Code	`WCHAR pathDir[] = L"C:\\ADirectory\\AnotherElement";`
	`LPCWSTR pszDir = pathdir;`
	`WCHAR name[]= L"A*Name??WithStuffTo::Remove.foo"; // Buffer size not large enough to be safe`
	`LPWSTR pszSpec = name;`
	`PathCleanupSpec(pszDir, pszSpec);`

Examples of Corrected Code	`WCHAR pathDir[] = L"C:\\ADirectory\\AnotherElement";`
	`LPCWSTR pszDir = pathdir;`
	`WCHAR name[MAX_PATH] = L"A*Name??WithStuffTo::Remove.foo"; // Note size is large enough`
	`LPWSTR pszSpec = name;`
	`PathCleanupSpec(pszDir, pszSpec);`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/pathcleanupspec.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com[1].

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com